REMARKS.

Claim Objections.

The Examiner has objected Claims 5-6 under 37 CFR 1.75(c). To meet the objection these two claims were rewritten as one new claim 5. The word "system" in this claim may refer, for example, to a system containing ATM, as it is explained in the end of Detailed Description of the Invention.

Claim Rejections.

A. Claim Rejections: claim by claim comparison

Below are the claim by claim differences between Buffam's invention and my application in view of the Examiner objections.

Claim 1. (Sampling):

Buffam extracts a set of true image points (TIP) from raw biometric data and generates a set of false image points (FIP). False image points are used to produce an encoding key.

My method does not generate false points, does not use a key, and does not encrypt the data. Instead it changes the order of the sequence of values in the array of the true biometric data, e.g. the original sequence of values 11, 12, 13, 15, 22 may be converted into sequence 12, 15, 13, 22, 11.

Claim 2. (Calculations on client).

In Buffam's invention, false image points are created and added to the true image points, the union of which is saved in the template.

In my method, no new data is added to the biometric template. Instead, true biometric data is registered as the sequence of values in an array and secret information known only to the user is used to shuffle the sequence of values in the biometric array, e.g. the original sequence of values 11, 12, 13, 15, 22 may be converted into sequence 12, 15, 13, 22, 11.

Claim 3. (Additional calculations on client).

In Buffam's invention, the encoding key is the result of imposing a hashing function on an ordered set of false image points. The key is used to encrypt plain text, and a portion of the resulting cipher text is added to the template. The template is saved in user's credentials.

In my method, the sequence of values in biometric array may be optionally multiplied by the sequence of numbers known to the user only, e.g. the sequence 12, 15, 13, 22, 11 may be transformed into sequence 234, -3, 14, 333, -72. The resulting sequence is saved in user's credentials.

Claim 4. (Verification).

In Buffam's invention the TIP of a claimant are removed from the saved user's credentials. The remaining set of image points is used to produce the decoding key and decrypt the cipher text. If the claimant is the correct person then the remaining set of image points is his FIP, so the decoding key is correct, the decrypted cipher text matches the plain text and authentication is provided.

In my method, there is no decoding. The twisted signature of a claimant received from the client side is compared with the twisted signature saved on the server, e g. with 234, -3, 14, 333, -72. If the claimant is the correct person, these signatures match. Because of the non-deterministic nature of biometric sampling calculation of correlation coefficient may be used instead of direct comparison.

Claim 5. (System and implementation).

Buffman claims the means for implementation of his method.

I claim the means for implementation of my method.

B. Claim Rejections: broad scope argument

The differences listed above are important in achieving the main goal of the invention - privacy of user.

With respect to Buffam's invention, let us assume that security of the server is compromised and that an attacker has possession of the following information:

- the union of the user's TIP and FIP,
- all calculation algorithms used in creation of FIP from TIP,
- all calculation algorithms used in creating an encoding key from FIP, and
- all calculation algorithms used to created the cipher text from the plain text

The true biometric information is still unknown (concealed in the union with false information).

One possible approach of an attacker is the trial and error method. The attacker selects several image points from the union of TIP and FIP, generates a key, and enters random plain text. If the resulting cipher text matches the saved cipher text, then the image points remaining in the union are the user's TIP. In this scenario, the user loses his biometrics privacy forever. The important part is that there is a clear criterion: the attacker stops the search when the produced cipher text coincides with the saved one.

Another possible approach of an attacker is the creation of new mathematical methods. "The existence of one-way functions is an open conjecture" (http://en.wikipedia.org/wiki/One-way_function) - their existence has not been proven and is an unsolved problem in computer science. In fact, another instrument, to which Buffam reffers to as the most secure algorithm and which had been commonly used and relied on in cryptography—MD5 hash function - has already been found to have weekness. "In August 2004, researchers found weaknesses in a number of hash functions, including MD5" (http://en.wikipedia.org/wiki/Cryptographic_hash_function). Thus, at least theoretically, it is not impossible that an attacker can create a new mathematical method and restore both the key and the true biometrics.

With respect to my application, let us also assume that security of the server is compromised and that an attacker has possession of

- the twisted signature (permutation of the values in real array of biometric data according to my invention) and
- the method by which real biometric data is permutated ("twisted").

The real biometric data (correct sequence of values in the biometric array) and the secret information used to twist it are unknown.

Since according to my method the order of sequence of values in biometric array is changed on the client side by the user, and is not exposed to the server, there is no

theoretical possibility of restoring initial order. The attacker has nothing to decode. He can change the order of values in the stolen twisted signature, but he does not have a criterion when to stop in order to have the real signature: he has nothing to compare his results with. So, the privacy of the user is assured in greater degree in my method.

I believe this difference presents patentable novelty which the claims present in view of the references cited (Buffam, US-6185316-B1) and the rejection made ("anticipation").

Inventor  V.Gorelik. 4/7/2007